WHAT IS CLAIMED IS:

1. A method of transmitting a message, the method comprising:

generating a random number according to a predetermined random number generation algorithm;

constructing a first security field including the random number;

encrypting the first security field to create a first digital signature;

appending the first digital signature to the message to create a packet; and

transmitting the packet including the first digital signature and the message.

2. The method of Claim 1, wherein constructing a first security field is preceded by computing a Cyclic Redundancy Check (CRC) for the message, and wherein constructing the first security field comprises constructing the first security field including the first random number and the CRC.

3. The method of Claim 2, wherein computing the CRC for the packet is followed by appending the CRC to the message so that the packet includes the message, the CRC, and the first security field.

4. The method of Claim 1, wherein the predetermined random number generation algorithm is advanced at the first station with the transmission of each packet.

5. A method of receiving a packet including a message and a first digital signature wherein the first digital signature is generated by constructing a first security field including a first random number generated according to a predetermined random number generation algorithm and encrypting the first security field, the method comprising:

receiving the packet including the first digital signature and the message;

generating a second random number according to the predetermined random number generation algorithm;

constructing a second security field including the second random number; and

comparing the second security field including the second random number and the first digital signature.

6. The method of Claim 5, wherein comparing the second security field comprises:

encrypting the second security field to create a second digital signature; and

comparing the first digital signature and the second digital signature.

7. The method of Claim 5, wherein comparing the second security field comprises:

unencrypting the first digital signature to obtain the first security field; and

comparing the first security field and the second security field.

8. The method of Claim 5, wherein the first security field includes the first random number and a first cyclic redundancy check for the message, and wherein constructing a second security field is preceded by:

computing a second Cyclic Redundancy Check for the message portion of the packet;

wherein constructing the second security field comprises constructing the second security field including the second random number and the second CRC.

9. The method of Claim 8, further comprising:

verifying validity of the message portion of the packet; and

rejecting the packet if the message is not valid.

10. The method of Claim 6, wherein comparing the first digital signature and the second digital signature is followed by:

determining if the first digital signature and the second digital signature are the same; and

rejecting the packet if the first digital signature and the second digital signature are not the same.

11. The method of Claim 5, wherein generating the first random number according to the predetermined random number generation algorithm and generating the second random number according to the predetermined random number generation algorithm are synchronized so that the first and second random numbers are the same.

12. The method of Claim 11, wherein the predetermined random number generation algorithm operates at both a first and a second station using a common seed to produce the same random number.

13. The method of Claim 5, wherein the predetermined random number generation algorithm is advanced at both a first and a second station with the transmission and reception of each packet.

14. A method of authenticating a message, the method comprising:

generating at a first station a first random number according to a predetermined random number generation algorithm;

constructing at the first station a first security field including the first random number;

encrypting the first security field to create a first digital signature;

appending the first digital signature to the message to create a packet;

transmitting the packet including the first digital signature and the message to a second station;

receiving the packet including the first digital signature and the message at the second station;

generating at the second station a second random number according to the predetermined random number generation algorithm;

constructing at the second station a second security field including the second random number; and

comparing the second security field including the second random number and the first digital signature.

15. The method of Claim 14, wherein comparing the second security field comprises:

encrypting the second security field to create a second digital signature; and

comparing the first digital signature and the second digital signature.

16. The method of Claim 14, wherein comparing the second security field comprises:

unencrypting the first digital signature to obtain the first security field; and

comparing the first security field and the second security field.

17. The method of Claim 14, wherein constructing at a first station a first security field is preceded by:

computing a Cyclic Redundancy Check (CRC) for the message;

wherein constructing the first security field comprises constructing the first security field including the first random number and the CRC.

18. The method of Claim 17, wherein computing the CRC for the packet is followed by:

appending the CRC to the message so that the packet includes the message, the CRC, and the first security field.

19. The method of Claim 14, wherein constructing at the second station a second security field is preceded by:

computing a second Cyclic Redundancy Check (CRC) for the message portion of the packet;

wherein generating at the second station the second security field comprises generating at the second station the second security field including the second random number and the second CRC.

20. The method of Claim 14, further comprising:

verifying validity of the message portion of the packet; and

rejecting the packet if the message is not valid.

21. The method of Claim 15, wherein comparing the first digital signature and the second digital signature is followed by:

determining if the first digital signature and the second digital signature are the same; and

rejecting the packet if the first digital signature and the second digital signature are not the same.

22. The method of Claim 14, wherein generating at the first station the first random number according to the predetermined random number generation algorithm and generating at the second station the second random number according to the predetermined random number generation algorithm are synchronized so that the first and second random numbers are the same.

23. The method of Claim 22, wherein the predetermined random number generation algorithm operates at both the first and second stations using a common seed to produce the same random number.

24. The method of Claim 14, wherein the predetermined random number generation algorithm is advanced at both the first and second stations with the transmission and reception of each packet.

25. A system for transmitting a message comprising:

a random number generator that generates a random number according to a predetermined random number generation algorithm;

a circuit that constructs a first security field including the random number, encrypts the first security field to create a digital signature, and appends the first digital signature to the message to create a packet; and

a transmitter that transmits the packet including the digital signature and the message.

26. The system according to Claim 25, wherein the circuit that constructs a first security field is configured to compute a Cyclic Redundancy Check (CRC) for the message, wherein the first security field includes the first random number and the CRC.

27. The system according to Claim 26, wherein the circuit that constructs the first security field is further configured to append the CRC to the message so that the packet includes the message, the CRC, and the first security field.

28. The system according to Claim 25, wherein the random number generator is configured to advance at the first station when the transmitter transmits each packet.

29. A system for receiving a packet including a message and a first digital signature wherein the first digital signature is generated by constructing a first security field including a first random number generated according to a predetermined random number generation algorithm and encrypting the first security field, the system comprising:

a receiver that receives the packet including the first digital signature and the message;

a second random number generator that generates a second random number according to the predetermined random number generation algorithm;

a second circuit that constructs a second security field including the second random number and compares the second security field including the second random number and the first digital signature.

30. The system according to Claim 29, wherein the second circuit encrypts the second security field to create a second digital signature, and compares the first digital signature and the second digital signature.

31. The system according to Claim 29, wherein the second circuit unencrypts the first digital signature to obtain the first security field, and compares the first security field and the second security field.

32. The system according to Claim 29, wherein the second circuit that constructs the second security field is configured to compute a second Cyclic Redundancy Check for the message portion of the packet, wherein the second security field includes the second random number and the second CRC.

33. The system according to Claim 32, wherein the second circuit that generates the second security field is further configured to verify validity of the message portion of the packet and reject the packet if the message is invalid.

34. The system according to Claim 29, wherein the second circuit that compares the first digital signature and the second digital signature is further configured to determine if the first digital signature and the second digital signature are the same and reject the packet if the first digital signature and the second digital signature are not the same.

35. The system according to Claim 29, wherein the first random number generator that generates the first random number according to the predetermined random number generation algorithm and the second random number generator that generates the second random number according to the predetermined random number generation algorithm are synchronized so that the first and second random numbers are the same.

36. The system according to Claim 35, wherein the first and second random number generators operate using a common seed to produce the same random number.

37. The system according to Claim 36, wherein first and second random number generators are advanced with the transmission and reception of the packet.

38. A computer program product for transmitting a message, comprising:

a computer readable program medium having computer readable code embodied therein, the computer readable code comprising:

computer readable program code that generates a random number according to a predetermined random number generation algorithm;

computer readable program code that constructs a first security field including the random number, encrypts the first security field to create a digital signature, and appends the first digital signature to the message to create a packet; and

computer readable program code that transmits the packet including the digital signature and the message.

39. The computer program product of Claim 38, wherein the computer readable program code that constructs the first security field is configured to compute

a Cyclic Redundancy Check (CRC) for the message, wherein the first security field includes the first random number and the CRC.

40. The computer program product of Claim 39, wherein the computer readable program code that constructs the first security field is further configured to append the CRC to the message so that the packet includes the message, the CRC, and the first security field.

41. The computer program product of Claim 38, wherein the predetermined random number generation algorithm is configured to advance at the first station when the transmitter transmits each packet.

42. A computer program product for receiving a packet including a message and a first digital signature wherein the first digital signature is generated by computer readable program code that constructs a first security field including a first random number according to a predetermined random number generation algorithm and encrypts the first security field, comprising:

a computer readable program medium having computer readable code embodied therein, the computer readable code comprising:

computer readable program code that receives the packet including the first digital signature and the message;

computer readable program code that generates a second random number according to the predetermined random number generation algorithm;

computer readable program code that constructs a second security field including the second random number and compares the second security field including the second random number to the first digital signature.

43. The computer program product of Claim 42, wherein the computer readable program code that compares the second security field is configured to encrypt the second security field to create a second digital signature and compare the first digital signature and the second digital signature.

44. The computer program product of Claim 42, wherein the computer readable program code that compares the second security field is configured to unencrypt the first digital signature to obtain the first security field and compare the first security field and the second security field.

45. The computer program product of Claim 42, wherein the computer readable program code that constructs the second security field is configured to compute a second Cyclic Redundancy Check for the message portion of the packet, wherein the second security field includes the second random number and the second CRC.

46. The computer program product of Claim 45, wherein the computer readable program code that constructs the second security field is further configured to verify validity of the message portion of the packet and reject the packet if the message is not valid.

47. The computer program product of Claim 42, wherein the computer readable program code that compares the first digital signature and the second digital signature is further configured to determine if the first digital signature and the second digital signature are the same and reject the packet if the first digital signature and the second digital signature are not the same.

48. The computer program product of Claim 47, wherein the computer readable program code that generates the first random number according to the predetermined random number generation algorithm and the computer readable program code that generates the second random number according to the predetermined random number generation algorithm are configured so that the first and second random numbers are the same.

49. The computer program product of Claim 48, wherein the predetermined random number generation algorithm is configured to operate at both the first and second stations using a common seed to produce the same random number.

50. The computer program product of Claim 42, wherein the predetermined random number generation algorithm is configured to advance with the transmission and reception of each packet.